AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of detecting denial of service (DoS) attacks in an ~~internet~~ Internet accessible network having at least one proxy server incorporating a session initiation protocol (SIP), said session initiation protocol includes INVITE (INV) messages that request set-up of an Internet telephone call and SIP 180 messages indicate ringing , comprising the steps of: detecting ~~any substantial~~ an imbalance between an accounting of said SIP INVITE ~~(INV)~~ and SIP 180 ~~(N_{180})~~ Ringing messages resulting from a denial of service attack; and providing an indication of the presence of a current DoS attack on said proxy server based on detection of said imbalance.

2. (Currently Amended) The method of detecting denial of service attacks in an ~~internet~~ Internet accessible network as defined in claim 1 wherein the number (H) of INVITE messages including credentials ~~(INV_c)~~ that are sent from a user client in response to an authentication required (407) message from the proxy server, said credentials being information used by the proxy server to authenticate the INVITE messages, are removed from the accounting before the balance is tested such that when the equation:

$$INV_o\ [[to]] + INV_c - H = N_{180}$$

where INV_o is the number of INVITE messages without said credentials, INV_c is the number of INVITE messages with said credentials, and N_{180} is the number of said 180 messages, is not true within a ~~small~~ predetermined margin of error, then the presence of a denial of service attack on the proxy server is indicated by the inequality.

3. (Currently Amended) The method of detecting denial of service attacks in an ~~internet~~ Internet accessible network as defined in claim 2 further including causing said proxy server to maintain a call information table for determining the value of H.

4. (Canceled)

5. (Currently Amended) A system for detecting denial of service attacks against session initiation protocol elements in ~~a internet~~ an Internet accessible network having at least one proxy server, ~~comprising means at~~ wherein said proxy server includes means for determining if the number of INVITE messages including credentials (INV_c) sent to said proxy server from user clients in response to an authentication requirement ~~and providing an indication of~~ exceeds a predetermined level that indicates a DoS attack ~~when the number of INVITE messages exceeds a predetermined level~~, said credentials being information used by the proxy server to authenticate the INVITE messages.

6. (Currently Amended) A system for detecting denial of service attacks in an ~~internet~~ Internet accessible network having at least one proxy server incorporating session initiation protocol (SIP), ~~comprising~~ wherein said proxy server ~~including~~ includes means for detecting ~~any substantial~~ an imbalance between an accounting of SIP INVITE ~~(INV)~~ and SIP 180 Ringing messages ~~and means providing indication of~~ that indicates the presence of a current denial of service attack on said proxy server.

7. (New) A system for detecting denial of service attacks against session initiation protocol elements in an Internet accessible network as claimed in claim 5, wherein said means creates a call-info table for use in tracking said INVITE messages.

8.(New) A system for detecting denial of service attacks against session initiation protocol elements in an Internet accessible network as claimed in claim 6, wherein said means creates a call-info table.